STATEMENT

OF

MARK MACCARTHY

ON BEHALF OF

VISA U.S.A. INC.

BEFORE THE

SUBCOMMITTEE ON

MANAGEMENT, INTEGRATION, AND OVERSIGHT

OF THE

COMMITTEE ON HOMELAND SECURITY

UNITED STATES HOUSE OF REPRESENTATIVES

The Need to Strengthen Information Security at the Department of Homeland Security

April 14, 2005

Mr. Chairman, my name is Mark MacCarthy. I am Senior Vice President for Public Policy for Visa U.S.A. Inc. Visa appreciates the opportunity to address the important issues raised by today's hearing on the need to strengthen information security.

The Visa Payment System, of which Visa U.S.A. is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud.

Visa commends the Subcommittee for focusing on the important issue of information security. As the leading consumer electronic commerce payment system in the world, Visa considers it a top priority to remain a leader in the development of technology, products, and services that protect consumers from the effects of information security breaches. As a result, Visa has long recognized the importance of strict internal procedures to protect the customer information of Visa's members, thereby protecting the integrity of the Visa system.

Visa has substantial incentives to maintain strong security measures to protect customer information and the Visa system overall. The Visa system provides for zero liability to cardholders for unauthorized customer transactions. Cardholders are not responsible for unauthorized use of their cards. The Visa Zero Liability policy guarantees maximum protection for Visa cardholders against fraud due to information security breaches. Because the financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholder customers, these institutions incur costs from fraudulent transactions. These costs are

in the form of direct dollar losses from credit that will not be repaid, and also can be in the form of indirect costs attributable to the harm and inconvenience that might be felt by customers or merchants. Accordingly, Visa aggressively protects the customer information of its members.

Visa's Cardholder Information Security Plan

Visa is currently implementing a comprehensive and aggressive customer information security program known as the Cardholder Information Security Plan ("CISP"). This security program applies to all entities, including merchants, that store, process, transmit, or hold Visa cardholder data, and covers enterprises operating through brick-and-mortar stores, mail and telephone order centers, or the Internet. CISP was developed to ensure that the customer information of Visa's members is kept protected and confidential. CISP includes not only data security standards but also provisions for monitoring compliance with CISP and sanctions for failure to comply.

As a part of CISP, Visa requires all participating entities to comply with the "Visa Digital Dozen"—twelve basic requirements for safeguarding accounts. These include: (1) install and maintain a working network firewall to protect data; (2) do not use vendor-supplied defaults for system passwords and security parameters; (3) protect stored data; (4) encrypt data sent across public networks; (5) use and regularly update anti-virus software; (6) develop and maintain secure systems and applications; (7) restrict access to data on a "need-to-know" basis; (8) assign a unique ID to each person with computer access; (9) restrict physical access to data; (10) track all access to network resources and data; (11) regularly test security systems and processes; and (12) implement and maintain an overall information security policy.

Audits

For the largest companies, those who process more than 6 million Visa transactions per year, we require an annual on-site audit validated by an independent security assessor, or an internal audit signed by an officer of the company. Visa also requires quarterly network scans validated by a qualified independent scan vendor. Visa provides lists of recommended security assessors, scan vendors, and software providers.

Sanctions

Visa takes enforcement action against companies that do not implement adequate security. Visa members are subject to fines, up to $500,000 per incident, for any merchant or service provider that is compromised and not CISP-compliant at the time of the incident.

Payment Card Industry Data Security Standard

Visa is not the only credit card organization that has developed security standards. In order to avoid the potential for imposing conflicting requirements on merchants and others, in December of 2004, Visa, MasterCard, American Express, Discover, and Diners Club collaborated to align their respective data security requirements for merchants and third parties. We found that the differences between these security programs were more procedural than substantive. Therefore, Visa has been able to integrate CISP into a common set of data security requirements without diluting the substantive measures for information security already developed in CISP. Visa supports this new, common set of data security requirements, which is known as the Payment Card Industry Data Security Standard ("PCI Standard").

The PCI Standard provides a common framework that encompasses four fundamental aspects of information security:

- **Technical Foundation**: The PCI Standard details technical requirements for the secure storage, processing, and transmission of cardholder data.

- **Testing Methodologies**: The PCI Standard promotes the development of common security auditing procedures, scanning procedures, and provides a common security Self-Assessment Questionnaire.

- **Vendor Certification**: The PCI Standard enables participants to cross-recognize their respective certifications for vendors. In particular, MasterCard has agreed to recognize Visa-approved onsite security assessors, and Visa will recognize MasterCard security scan vendors.

- **Compliance Validation**: The individual security programs maintained by payment card systems, such as Visa's CISP or MasterCard's security program, have been restructured within the framework of the PCI Standard so that each has similar merchant and service provider-levels and validation requirements.

The new alignment of security standards under this framework allows merchants and service providers to select one vendor and implement a single process to comply with all payment card data security programs. Instead of fragmenting their resources to satisfy separate requirements, the PCI Standard allows merchants and service providers to focus on achieving a common objective: robust and continuously upgraded security programs.

Neural Networks to Detect Fraud and Block Potentially Unauthorized Transactions

In addition to the CISP program, Visa uses sophisticated neural networks that flag unusual spending patterns for fraud and block the authorization of transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institution and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of cards, we again notify the issuing institutions, who begin a process of investigation and card re-issuance.

Mr. Chairman, Visa has additional information about its programs to prevent identity theft and to aid customers to recover from identity theft. I respectfully request that information relating to these programs, and to the programs which I have described in my testimony, be included in the record of this hearing.

Thank you, again, for the opportunity to present this testimony today. I would be happy to answer any questions.